# Process for the control of secret keys between two smart cards

Patent Number: US5602915
Publication date: 1997-02-11
Inventor(s): CAMPANA MIREILLE (FR); GILBERT HENRI (FR); ARDITTI DAVID (FR)
Applicant(s):: FRANCE TELECOM (FR)
Requested Patent: EP0613105, B1
Application Number: US19940201979 19940225
Priority Number(s): FR19930002152 19930225
IPC Classification: H04L9/08 ; H04L9/00
EC Classification: G07F7/10D4E2, H04L9/08
Equivalents: DE69408176D, DE69408176T, FR2702066

## Abstract

A process for controlling communication between a first and a second smart card using key-based cryptography is provided. In the disclosed process, a first identity code is stored in the first smart card and a second identity code is stored in the second smart card. The smart cards are customized by writing into each of the smart cards an identical group secret key and respective algorithms for processing the identical group secret key and the first and second identity codes stored in the first and second smart cards, respectively. The smart cards are used by transmitting the first identity code to the second smart card, transmitting the second identity code to the first smart card, and calculating using the respective processing algorithms stored in the smart cards, first and second session keys for the first and second smart cards, respectively.

Data supplied from the **esp@cenet** database - I2

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Übersetzung der europäischen Patentschrift

(87) EP 0 613 105 B1

(10) DE 694 08 176 T 2

(51) Int. Cl.[6]: G 07 F 7/10

(21) Deutsches Aktenzeichen: 694 08 176.0
(86) Europäisches Aktenzeichen: 94 400 386.2
(86) Europäischer Anmeldetag: 23. 2. 94
(87) Erstveröffentlichung durch das EPA: 31. 8. 94
(87) Veröffentlichungstag der Patenterteilung beim EPA: 28. 1. 98
(47) Veröffentlichungstag im Patentblatt: 30. 7. 98

(30) Unionspriorität:
9302152 25. 02. 93 FR

(73) Patentinhaber:
France Télécom, Paris, FR

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, Anwaltssozietät, 80538 München

(84) Benannte Vertragstaaten:
DE, GB

(72) Erfinder:
Campana, Mireille, F-92140 Clamart, FR; Gilbert, Henri, F-91440 Bures sur Yvette, FR; Arditti, David, F-92140 Clamart, FR

(54) Verwaltungsverfahren von Geheimschlüsseln zwischen zwei Chipkarten

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patentamt inhaltlich nicht geprüft.

94 400 386.2
FRANCE TELECOM

Gebiet der Erfindung

Die Erfindung betrifft ein Verfahren zum Verwalten der Geheimschlüssel zwischen zwei Chipkarten.

Die Chipkarten entwickeln sich gegenwärtig sehr stark als Daten-Authentifizierungs- und -Zertifizierungsmittel, insbesondere aufgrund ihrer Fähigkeit, Geheimdaten zu speichern.

Das Gebiet der Erfindung umfaßt alle diese zur Daten-Authentifizierung und -Zertifizierung benutzten Kartentypen, die dazu bestimmt sind, durch ein Informatiksytem gelesen zu werden, das einen Chipkarten-Leser umfaßt. Diese Chipkarten können z.B. Terminalkarten wie die Telekopierer- oder Bankomat-Chipkarten sein, die mittels eines Durchschalt- bzw. Wahlnetzwerks dialogieren.

Diese Chipkarten werden in der Folge einfach "Karten" genannt.

Stand der Technik

Bei den meisten Karten-Informatiksystemen ist es üblich, einen zentralen Informatik-Server zu verwenden, der fähig ist, "Mutterkarten" genannte Chipkarten zu lesen. An diesen zentralen Server sind eine Vielzahl von Informatikterminals angeschlossen, die "Tochterkarten" genannte Sekundärkarten lesen können. Diese Terminals sind dann einer sternförmigen Architektur entsprechend an den zentralen Server angeschlossen. Nach dieser sternförmigen Architektur kann der Dialog nur zwischen der Mutterkarte und einer der Tochterkarten hergestellt werden. Zwei Tochterkarten können nicht miteinander dialogieren, d.h. untereinander Daten austauschen.

Ein Informatiksystem mit einer derartigen Architektur ermöglicht auch, gesicherte Transaktionen zwischen den Tochterkarten und der Mutterkarte durchzuführen, aber es

ermöglicht keine gesicherte gegenseitige Transaktion zwischen zwei Tochterkarten.

Ein solches Informatiksystem hat ebenfalls den Nachteil, daß beim Erstellen eines gemeinsamen Sessions- bzw. Sitzungsschlüssels zwischen zwei Karten jede dieser Karten einen persönlichen Geheimschlüssel besitzt, der mit dem Geheimschlüssel der anderen Karte, mit der man einen gemeinsamen Sessionsschlüssel erstellen möchte, identisch ist.

Ein solches Informatiksystem mit einer Mikroprozessorkarte, die einen kryptographischen Algorithmus anwendet, wird in den französischen Patentanmeldungen FR-2 601 795 und FR-2 469 760 beschrieben. Diese Patentanmeldungen beschreiben nämlich Vorrichtungen, die ein Dialogverfahren zwischen einer Mutterkarte und Tochterkarten anwenden, die als sternförmiges Netz organisiert sind. Die durch diese Verfahren durchführbaren Operationen können folglich zwischen einer Mutterkarte und den Tochterkarten nur mit Hilfe der Geheimschlüssel durchgeführt werden, die man durch Diversifikation des Mutter-Schlüssels (Geheimschlüssel der Mutterkarte) erhält. Jeder derart erhaltene Geheimschlüssel ist das Resultat einer Berechnung, wobei der Mutterschlüssel und ein Eigenparameter derjenigen Tochterkarte verrechnet werden, mit der die Mutterkarte dialogieren will. Ein solches Informatiksystem ermöglicht folglich nicht das Durchführen eines Verfahrens, das einen gemeinsamen Sessionsschlüssel zwischen zwei Tochterkarten benutzt.

Andere klassische Informatiksysteme werden insbesondere in dem Dokument EP-A-0 422 230 beschrieben.

Durch dieses Dokument EP-A-0 422 230 kennt man ein Verwaltungsverfahren von Geheimschlüsseln zwischen einer ersten und einer zweiten Chipkarte, bei dem ein erster Identitätscode in der ersten Karte abgespeichert ist und ein zweiter Identitätscode in der zweiten Karte abgespeichert ist und das durch die folgenden Phasen gebildet wird:

- eine Personalisierungsphase, folgende Schritte umfassend:
  - Einschreiben desselben Gruppengeheimschlüssels in jede der Chipkarten;

- Einschreiben eines Verarbeitungsalgorithmus des Gruppengeheimschlüssels und der Identitätscodes in jede der Chipkarten;

· eine Benutzungsphase, folgende Schritte umfassend:

- Übertragen des ersten Identitätscodes zur zweiten Chipkarte;
- Übertragen des zweiten Identitätscodes zur ersten Chipkarte;
- Berechnen, durch die Verarbeitungsalgorithmen, eines ersten und eines zweiten Sessions- bzw. Sitzungsschlüssels jeweils in der ersten und der zweiten Chipkarte.

Ein weiteres bekanntes Informatiksystem wird in einem kurzen kommerziellen Hinweis der gemeinsamen Zentrale von FRANCE TELECOM und von TDF, CCETT beschrieben. Dieses Informatiksystem umfaßt eine Multiservice-Mikroprozessorkarte, bekannt unter der Handelsbezeichnung "Mimosa" ®. Eine solche Multiservice-Mikroprozessorkarte benutzt einen Algorithmus mit öffentlichem Schlüssel. Zwei Karten dieses Typs sind fähig, sich gegenseitig zu authentifizieren. Sie können Signaturen aussenden und zertifizieren, indem sie den Algorithmus mit öffentlichem Schlüssel benutzen, der auf der Identität beruht. Ein solcher Algorithmus mit öffentlichem Schlüssel ermöglicht ebenfalls das Erstellen eines Sessionsschlüssels zwischen zwei Karten. Dieser Algorithmus wendet auf Zahlen von mehreren hundert Bits arithmetische Operationen an (Multiplikationen, Potenzen, Divisionen), wobei diese Rechenkomplexität zur Folge hat, daß die Herstellung dieser Karten Hochleistungskomponenten erforderlich macht, die gegenwärtig noch sehr teurer sind.

## Darstellung der Erfindung

Die Aufgabe der vorliegenden Erfindung besteht darin, die Nachteile der vorhergehend beschriebenen Informatiksysteme zu beseitigen, indem sie ein Geheimschlüssel-Verwaltungsverfahren vorschlägt, dessen Anwendung einfach und relativ kostengünstig ist.

Zu diesem Zweck hat sie ein Geheimschlüssel-Verwaltungsverfahren zwischen zwei Chipkarten zum Gegenstand, bei

dem ein erster Identitätscode in der ersten Chipkarte abgespeichert ist und ein zweiter Identitätscode in der zweiten Chipkarte abgespeichert ist. Dieses Verfahren wird durch die folgenden Phasen gebildet:

- eine Personalisierungsphase, folgende Schritte umfassend:
  - Einschreiben eines Verarbeitungsalgorithmus des Gruppengeheimschlüssels und der Identitätscodes in jede der Chipkarten;
  - Einschreiben desselben Gruppengeheimschlüssels in jede der Chipkarten;

- eine Benutzungsphase, folgende Schritte umfassend:
  - Übertragung des ersten Identitätscodes zur zweiten Chipkarte;
  - Übertragung des zweiten Identitätscodes zur ersten Chipkarte;
  - Übertragung derselben Zufallszahl zu jeder Chipkarte;
  - Berechnung, durch den Verarbeitungsalgorithmus, eines ersten und eines zweiten Sessionsschlüssels, jeweils in der ersten und der zweiten Chipkarte, in jeder der Chipkarten aus folgenden Schritten bestehend:
  - Anwendung eines Diversifikationsalgorithmus aufgrund des ersten und zweiten Identitätscodes und des Gruppengeheimschlüssels, um eine Geheimzahl zu bestimmen;
  - Anwendung eines Sessionsschlüssel-Berechnungsalgorithmus aufgrund der Zufallszahl und der Geheimzahl.

Nach einer Ausführungsart der Erfindung besteht der Diversifikationsalgorithmus darin:

- eine erste Geheimzahl festzulegen aufgrund des ersten Identitätscodes und des in jeder Chipkarte gespeicherten Gruppengeheimschlüssels,
- eine zweite Geheimzahl festzulegen aufgrund des zweiten Identitätscodes und des Gruppengeheimschlüssels,
- durch eine kommutative Operation die erste und die zweite Geheimzahl zu kombinieren, um die Geheimzahl zu erhalten, wobei diese kommutative Operation eine Addition sein kann.

Nach der bevorzugten Ausführungsart der Erfindung sind der Diversifikationsalgorithmus und der Sessionsschlüssel-Berechnungsalgorithmus der ersten und der zweiten Chipkarte identisch, wobei die für die erste und die zweite Chipkarte erhaltenen Sessionsschlüssel dann identisch sind.

Dieses Verfahren hat folglich den Vorteil, daß zwei Chipkarten fähig sind, miteinander zu dialogieren und sich durch Benutzung ihres Sessionsschlüssels bei einer Authentifizierungsoperation gegenseitig zu authentifizieren.

Da außerdem nur die Identitätscodes von einer Karte zur anderen übertragen werden, könnte ein Eindringling, der die Kommunikationen zwischen den beiden Karten überwacht, den Sessionsschlüssel am Ende des Protokolls nicht wiederherstellen, da dieser Eindringling durch das Abhören nicht den Gruppengeheimschlüssel kennen kann, da dieser zwischen den Karten nicht übertragen wird.

Dieses Verfahren hat ebenfalls den Vorteil, daß eine andere Karte mit demselben Gruppengeheimschlüssel wie die kommunizierenden Karten den Sessionsschlüssel dieser Karten nicht bestimmen kann, da dieser Schlüssel von den beiden Identitätscodes abhängt, von denen der eine notwendigerweise in der Karte abgespeichert ist.

## Kurze Beschreibung der Zeichnung

Die beigefügte einzige Figur stellt das Funktionsschema zur Erstellung eines zwei Chipkarten gemeinsamen Sessionsschlüssels dar.

## Detaillierte Darstellung von Ausführungsarten der Erfindung

In der Figur ist das Funktionsschema der Erstellungsoperation des den beiden Chipkarten C1 und C2 gemeinsamen Sessionsschlüssels dargestellt. Zum besseren Verständnis der Erfindung ist der mittels der Karte C1 erstellte Sessionsschlüssel mit S1 bezeichnet und der mittels der Karte C2 erstellte Sessionsschlüssel mit S2. Um derartige Sessionsschlüssel S1 und S2 zu erstellen, liefert das Informatiksystem an jede der Karten C1 und C2 eine Zufallszahl NA. Außerdem gehört jede der Karten zu einer Gruppe, d.h. daß jede der Karten zu einem System von Karten

gehört, die miteinander kommunizieren müssen. Noch genauer: eine Gruppe stellt die Gesamtheit der Korrespondenten dar, die miteinander kommunizieren müssen, wobei diese Kommunikation paarweise erfolgt und geschützt ist gegenüber den anderen Korrespondenten der Gruppe und gegenüber Korrespondenten außerhalb der genannten Gruppe. Jede der Chipkarten C1 und C2 besitzt außer dieser vom System empfangenen Zufallszahl NA einen Gruppengeheimschlüssel, mit G bezeichnet. Dieser Gruppengeheimschlüssel ist identisch für jede der Karten derselben Gruppe.

Außerdem besitzt jede der Karten dieser Gruppe (nämlich die Karten C1 und C2 in der Figur) einen persönlichen Identitätsschlüssel, für die Karte C1 mit ID1 bezeichnet und für die Karte C2 mit ID2. Die Identitätscodes ID1 und ID2 können, da sie nicht geheim sind, von einer Karte zur einer anderen übermittelt werden. In der Figur wird der Identitätscode ID1 zur Karte C2 übertragen und der Identitätscode ID2 zur Karte C1.

Außerdem sind in jeder dieser Karten C1 und C2 kryptographische Algorithmen eingespeichert, jeweils mit D1 und CC1 und D2 und CC2 bezeichnet.

Es wird also der durch die Karte C1 zur Karte C2 übertragene Identitätscode ID1 in den Diversifikationsalgorithmus D2 eingespeist, der in der Chipkarte C2 gespeichert ist. Der Diversifikationsalgorithmus D2 bestimmt aufgrund des so erhaltenen Identitätscodes ID1 und des Gruppengeheimschlüssels G eine erste Geheimzahl NS1. NS1 wird unter der Form NS1 = D2 (G, ID1) ausgedrückt.

Parallel dazu bestimmt dieser Diversifikationsalgorithmus D2 aus dem Identitätscode ID2 und dem Gruppengeheimschlüssel G eine zweite Geheimzahl NS2. Diese zweite Geheimzahl hat die Form NS2 = D2 (G, ID2).

Wenn die beiden Geheimzahlen NS1 und NS2 durch den Algorithmus D2 bestimmt worden sind, gewährleistet eine Add-Funktion die Addition dieser beiden Geheimzahlen NS1 und NS2. Die aus dieser Addition resultierende Geheimzahl wird mit NS bezeichnet.

Der Schlüsselberechnungsalgorithmus CC2 benutzt dann die derart berechnete Geheimzahl NS und ebenfalls die durch das

Informatiksystem gelieferte Zufallszahl NA, um den Sessionsschlüssel S2 der Speicherkarte C2 zu erzeugen.

Diese Diversifikations- und Schlüsselberechnungsalgorithmen D2 und CC2 werden nicht näher beschrieben, denn sie sind dem Fachmann bekannt und in den oben genannten Patentanmeldungen beschrieben.

Alle für die Karte C2 beschriebenen Operationen werden symmetrisch durch die Karte C1 ausgeführt.

So berechnet der in der Karte C1 gespeicherte Diversifikationsalgorithmus die erste Geheimzahl NS1 = D1(G, ID1), indem er den zu ihr gehörenden Identitätscode ID1 und den Gruppengeheimschlüssel G benutzt. Derselbe Diversifikationsalgorithmus D1 berechnet andererseits die Geheimzahl NS2 = D1(G, ID2), wobei er den von der Karte C2 empfangenen Identitätscode ID2 und den Gruppengeheimschlüssel G benutzt. Diese beiden Geheimzahlen NS1 und NS2 werden genauso wie in der Karte C1 durch eine Add-Funktion (oder irgendeine kommutative Operation) addiert, um die Geheimzahl NS zu liefern. Der Schlüsselberechnungsalgorithmus CC1 berechnet dann den Sessionsschlüssel S1 aus der vom Informatiksystem erhaltenen Zufallszahl NA und der Geheimzahl NS, berechnet wie vorhergehend beschrieben.

Zum besseren Verständnis der Erfindung wurden die Diversifikationsalgorithmen vorhergehend mit D1 und D2 bezeichnet; sie sind jedoch identisch. Dasselbe gilt für die Schlüsselberechnungsalgorithmen CC1 und CC2, die ebenfalls identisch sind. Man begreift, daß logischerweise, wenn die Algorithmen D1 und D2 und CC1 und CC2 jeweils identisch sind, die Sessionsschlüssel, mit der Bezeichnung S1 für den durch die Karte C1 erhaltenen Schlüssel und S2 für den durch die Karte C2 erhaltenen Schlüssel, ebenfalls identisch sind. Man hat also für die beiden Karten C1 und C2 einen gemeinsamen Sessionsschlüssel.

Durch die Lektüre dieser Beschreibung wird auch klar, daß jede Karte, die den Gruppengeheimschlüssel G besitzt, einen gemeinsamen Sessionsschlüssel mit jeder beliebigen anderen Karte derselben Gruppe erstellen kann, d.h. jeder den Geheimschlüssel G besitzenden Karte.

94 400 386.2
FRANCE TELECOM

## PATENTANSPRÜCHE

1. Verwaltungsverfahren von Geheimschlüsseln zwischen einer ersten und einer zweiten Chipkarte ($C_1$, $C_2$), bei dem ein erster Identitätscode (ID1) in der ersten Chipkarte gespeichert ist und ein zweiter Identitätscode (ID2) in der zweiten Chipkarte gespeichert ist,
gebildet durch die folgenden Phasen:

- eine Personalisationsphase, folgende Schritte umfassend:
  - Einschreiben desselben Gruppengeheimschlüssels in jede der Chipkarten;
  - Einschreiben eines Verarbeitungsalgorithmus des Gruppengeheimschlüssels und der Identitätscodes in jede der Chipkarten;
- eine Benutzungsphase, folgende Schritte umfassend:
  - Übertragen des ersten Identitätscodes (ID1) zur zweiten Chipkarte (C2);
  - Übertragen des zweiten Identitätscodes (ID2) zur ersten Chipkarte (C1);
  - Übertragen von ein und derselben Zufallszahl (NA) zu jeder der Chipkarten;

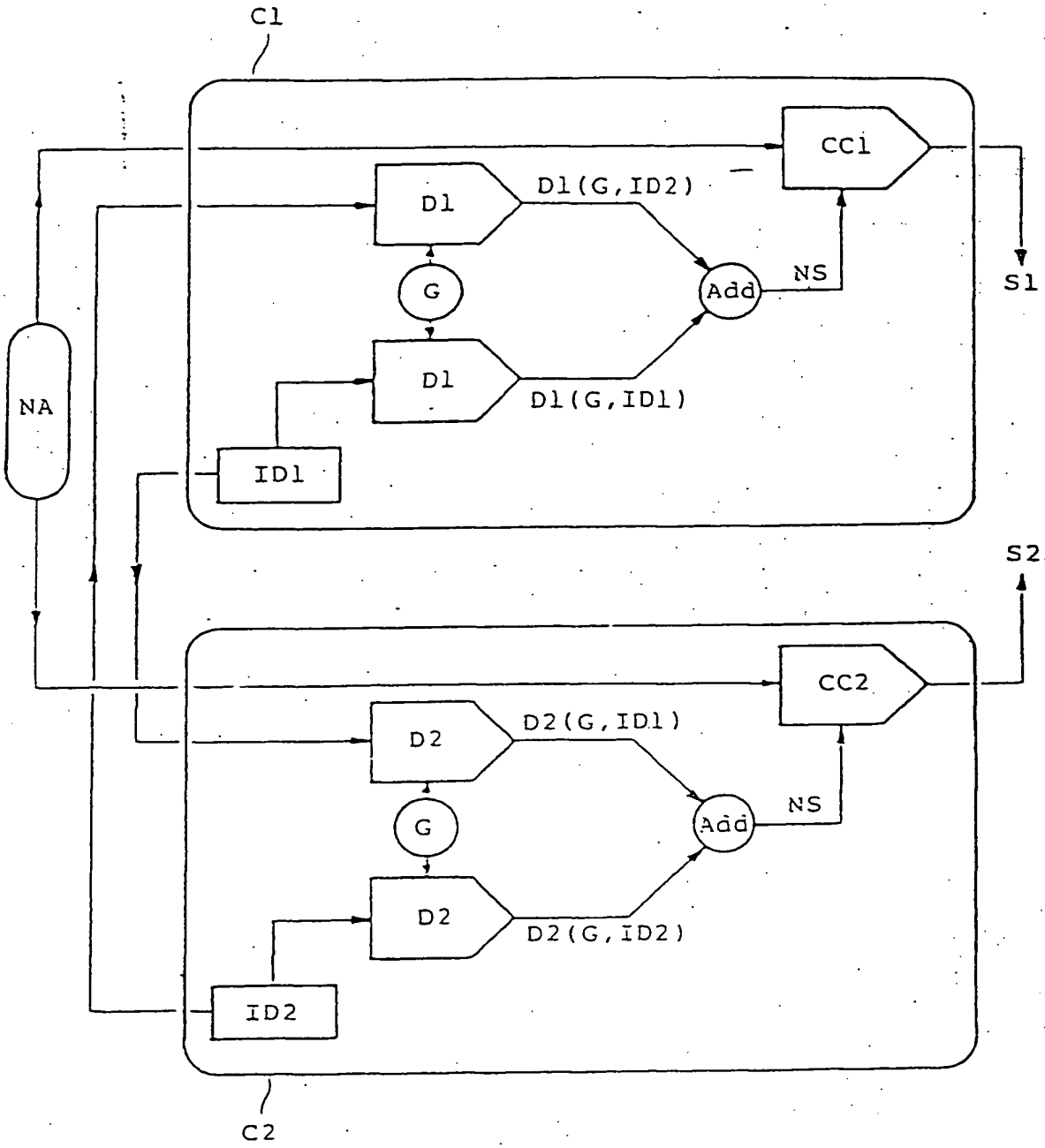
  - Berechnen, durch die Verarbeitungsalgorithmen, eines ersten und eines zweiten Sessions- bzw. Sitzungsschlüssels (S1, S2), jeweils in der ersten und der zweiten Chipkarte, in jeder der Chipkarten bestehend aus den Schritten:
  - Anwendung eines Diversifikationsalgorithmus (D1, D2) aufgrund des ersten und zweiten Identitätscodes (ID1, ID2) und des Gruppengeheimschlüssels, um eine Geheimzahl (NS) zu bestimmen;
  - Anwendung eines Sitzungs- bzw. Sessionsschlüssel-Berechnungsalgorithmus (CC1, CC2) aus der Zufallszahl (NA) und der Geheimzahl (NS).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Diversifikationsalgorithmus darin besteht:

- eine erste Geheimzahl (NS1) festzulegen aufgrund des ersten Identitätscodes (ID1) und des in jeder Chipkarte gespeicherten Gruppengeheimschlüssels,
- eine zweite Geheimzahl (NS1) festzulegen aufgrund des zweiten Identitätscodes (ID2) und des Gruppengeheimschlüssels,
- durch eine kommutative Operation die erste und die zweite Geheimzahl zu kombinieren, um die Geheimzahl (NS) zu erhalten.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die kommutative Operation, durchgeführt mit der ersten und zweiten Geheimzahl (NS1, NS2), in dem Diversifikationsalgorith-mus eine Addition ist.

4. Verfahren nach einem der Ansprüche 1 und 2, dadurch gekennzeichnet, daß der Diversifikationsalgorithmus (D1, D2) und der Sessionsschlüssel-Berechnungsalgorithmus (CC1, CC2) der ersten und der zweiten Chipkarte identisch sind, wobei die für die erste und die zweite Chipkarte erhaltenen Sessionsschlüssel dann identisch sind.


C1
CC1
D1
D1(G,ID2)
G
Add
NS
S1
D1
D1(G,ID1)
NA
ID1
S2
CC2
D2
D2(G,ID1)
G
Add
NS
D2
D2(G,ID2)
ID2
C2